PATENT OFFICE
JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy of the following application as filed with this office.

Date of Application: August 30, 1999

Application Number: Japanese Patent Application No. 11-243564

Applicant(s): NIPPON TELEGRAPH AND TELEPHONE CORPORATION
NEW MEDIA DEVELOPMENT ASSOCIATION

September 8, 2000

Commissioner,
Patent Office Kouzo Oikawa (Seal)

Certificate No.2000-3071368

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９９年　８月３０日

出願番号
Application Number: 平成１１年特許願第２４３５６４号

出願人
Applicant (s): 日本電信電話株式会社
財団法人ニューメディア開発協会

CERTIFIED COPY OF
PRIORITY DOCUMENT

２０００年　９月　８日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２０００－３０７１３６８

【書類名】　特許願

【整理番号】　NTTH115954

【提出日】　平成11年 8月30日

【あて先】　特許庁長官　伊佐山　建志　殿

【国際特許分類】　G06F 19/00

【発明者】

【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

【氏名】　赤鹿　秀樹

【発明者】

【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

【氏名】　平田　真一

【発明者】

【住所又は居所】　神奈川県川崎市川崎区観音二丁目３番９号

【氏名】　大山　永昭

【発明者】

【住所又は居所】　東京都港区三田一丁目４番２８号　財団法人　ニューメディア開発協会内

【氏名】　国分　明男

【特許出願人】

【識別番号】　000004226

【氏名又は名称】　日本電信電話株式会社

【特許出願人】

【識別番号】　596062738

【氏名又は名称】　財団法人ニューメディア開発協会

【代理人】

【識別番号】　100070150

【弁理士】

【氏名又は名称】　伊東　忠彦

【手数料の表示】

【予納台帳番号】　002989

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　データ格納システム及びデータ格納プログラムを格納した記憶媒体

【特許請求の範囲】

【請求項１】　データを格納する利用者装置と、該利用者装置の提供及び登録証を発行・管理する発行機関が有する発行装置と、データを提供するデータ提供機関が有するデータ提供装置、発行機関を登録・管理する発行登録機関が有する発行登録装置と、該データ提供機関を登録・管理するデータ登録機関が有するデータ登録装置からなるデータ格納システムにおいて、

前記利用者装置は、

利用者公開鍵を含む鍵に関する情報である登録情報を生成し、利用者情報と共に前記発行装置へ送信する登録情報生成手段と、

前記発行装置から取得した、前記登録情報及び前記利用者情報に対する発行機関の署名情報である登録証を検証し、検証結果が正しければ該登録証を記憶手段に記憶する登録証検証手段とを有し、

前記発行装置は、

前記登録証を生成し、前記利用者装置に送信する登録証生成手段とを有することを特徴とするデータ格納システム。

【請求項２】　前記利用者装置は、

前記登録証と格納データ情報を前記発行装置に送信する手段と、

前記発行装置から格納許可証を取得すると、該格納許可証を検証し、取得した格納データと、送信した前記格納データ情報との対応付けを検証し、検証結果が正しければ該格納データを記憶手段に格納する手段とを有し、

前記発行装置は、

前記利用者装置から受信した前記登録証と前記格納データ情報を検証し、検証結果が正しければ、前記登録証及び前記格納データに対して、証明情報を付与し、格納許可依頼を生成し、該登録証、該格納データ及び格納許可情報を前記データ提供装置に送信する手段と、

前記データ提供装置から取得した格納許可証を検証し、検証結果が正しければ

該格納許可証を前記利用者装置に送信する手段とを有し、

前記データ提供装置は、

前記格納許可情報を検証し、検証結果が正しければ前記格納許可依頼及び格納データ情報に対して証明情報を付与し、格納許可証を生成し、該格納許可証を前記発行装置に送信する手段を有する請求項１記載のデータ格納システム。

【請求項３】　前記利用者装置は、

前記登録証、前記格納データ情報を前記データ提供装置に送信する手段と、

前記データ提供装置から格納許可証を取得し、該格納許可証を検証し、取得した格納データと前記格納データ情報との対応付けを検証し、検証結果が正しければ該格納データを記憶手段に格納する手段とを有し、

前記データ提供装置は、

前記利用者装置から取得した前記登録証及び前記格納データ情報を検証し、検証結果が正しければ、該登録証及び該格納データ情報に対して証明情報を付与し、格納許可依頼を作成し、該登録証、該格納データ及び該格納許可依頼を前記発行装置に送信する手段と、

前記発行装置から取得した格納許可証を検証し、検証結果が正しければ、該格納許可証を前記利用者装置に送信する手段を有し、

前記発行装置は、

前記格納許可依頼を検証し、検証結果が正しければ、該格納許可依頼及び前記格納データ情報に対して証明情報を付与して、格納許可証を生成し、該格納許可情報をデータ提供装置に送信する手段を有する請求項１記載のデータ格納システム。

【請求項４】　前記利用者装置は、

前記登録証、前記格納データ情報を前記データ提供装置に送信する手段と、

前記データ提供装置から受信した格納許可証を検証し、取得した格納データと前記格納データ情報との対応付けを検証し、検証結果が正しければ、該格納データを記憶手段に格納する手段とを有し、

前記データ提供装置は、

前記利用者装置から取得した前記登録証を検証し、検証結果が正しければ該登

録証及び前記格納データ情報に対して証明情報を付与した格納許可証を生成し、該利用者装置に送信する手段を有する請求項１記載のデータ格納システム。

【請求項５】　前記発行装置は、

証明情報を付与するために用いる情報を前記発行登録装置に送信する手段と、

前記発行登録装置より取得した発行機関登録証を検証し、検証結果が正しければ、該発行機関登録証を格納しておく手段と、

前記利用者装置に対して前記登録証を生成し、該発行機関登録証と共に該利用者装置に送信する手段とを有し、

前記発行登録装置は、

前記発行装置から受信した前記証明情報を付与するために用いる情報に対して証明情報を付与し、発行機関登録証を作成し、前記発行装置に送信する手段を有し、

前記利用者装置は、

前記発行装置から取得した、前記登録証と前記発行機関登録証の両者を検証し、検証結果が正しければ該登録証及び前記発行機関登録証を記憶装置に格納する手段とを有する請求項１記載のデータ格納システム。

【請求項６】　前記データ提供装置は、

証明情報を付与するために用いる情報を前記データ登録装置に送信する手段と、

前記データ登録装置から受信したデータ提供機関登録証を検証し、検証結果が正しければ該データ提供機関登録証を格納する手段と、

利用者が格納する格納データに対して証明情報を付与して証明情報付き格納データとし、該証明情報付き格納データに前記データ提供機関登録証を付加する手段とを有し、

前記データ登録装置は、

前記データ提供装置から取得した前記証明情報を付与するために用いる情報に対して証明情報を付与したデータ提供機関登録証を作成して前記データ提供装置に送信する手段を有し、

前記利用者装置は、

前記データ提供装置から取得した前記証明情報付き格納データを前記データ提供機関登録証を用いて検証し、検証結果が正しければ前記格納データを前記記憶手段に格納する手段を有する請求項２、３、または、４記載のデータ格納システム。

【請求項７】　前記利用者装置は、

前記格納データを格納する代わりに、既に前記記憶手段内にある格納データを削除する手段を有する請求項２、３、または、４記載のデータ格納システム。

【請求項８】　データを格納する利用者装置と、該利用者装置の提供及び登録証を発行・管理する発行機関が有する発行装置と、データを提供するデータ提供機関が有するデータ提供装置、発行機関を登録・管理する発行登録機関が有する発行登録装置と、該データ提供機関を登録・管理するデータ登録機関が有するデータ登録装置からなるシステムにおいて、該利用者装置、該発行装置、該データ提供装置、該発行登録装置、及びデータ登録装置の各々に搭載されるデータ格納プログラムを格納した記憶媒体であって、

前記利用者装置に搭載される、

利用者公開鍵を含む鍵に関する情報である登録情報を生成し、利用者情報と共に前記発行装置へ送信させる登録情報生成プロセスと、

前記発行装置から取得した、前記登録情報及び前記利用者情報に対する発行機関の署名情報である登録証を検証し、検証結果が正しければ該登録証を記憶手段に記憶する登録証検証プロセスと、

前記発行装置に搭載される、

前記登録証を生成し、前記利用者装置に送信させる登録証生成プロセスとを有することを特徴とするデータ格納プログラムを格納した記憶媒体。

【請求項９】　前記利用者装置に搭載される、

前記登録証と格納データ情報を前記発行装置に送信させるプロセスと、

前記発行装置から格納許可証を取得すると、該格納許可証を検証し、取得した格納データと、送信した前記格納データ情報との対応付けを検証し、検証結果が正しければ該格納データを記憶手段に格納するプロセスと、

前記発行装置に搭載される、

前記利用者装置から受信した前記登録証と前記格納データ情報を検証し、検証結果が正しければ、前記登録証及び前記格納データに対して、証明情報を付与し、格納許可依頼を生成し、該登録証、該格納データ及び格納許可情報を前記データ提供装置に送信させるプロセスと、

前記データ提供装置から取得した格納許可証を検証し、検証結果が正しければ該格納許可証を前記利用者装置に送信させるプロセスと、

前記データ提供装置に搭載される、

前記格納許可情報を検証し、検証結果が正しければ前記格納許可依頼及び格納データ情報に対して証明情報を付与し、格納許可証を生成し、該格納許可証を前記発行装置に送信させるプロセスを有する請求項８記載のデータ格納プログラムを格納した記憶媒体。

【請求項１０】　前記利用者装置に搭載される、

前記登録証、格納データ情報を前記データ提供装置に送信させるプロセスと、

前記データ提供装置から格納許可証を取得し、該格納許可証を検証し、取得した格納データと前記格納データ情報との対応付けを検証し、検証結果が正しければ該格納データを記憶手段に格納するプロセスと、

前記データ提供装置に搭載される、

前記利用者装置から取得した前記登録証及び前記格納データ情報を検証し、検証結果が正しければ、該登録証及び該格納データ情報に対して証明情報を付与し、格納許可依頼を作成し、該登録証、該格納データ及び該格納許可依頼を前記発行装置に送信させるプロセスと、

前記発行装置から取得した格納許可証を検証し、検証結果が正しければ、該格納許可証を前記利用者装置に送信させるプロセスと、

前記発行装置に搭載される、

前記データ提供装置から取得した前記格納許可依頼を検証し、検証結果が正しければ、該格納許可依頼及び前記格納データ情報に対して証明情報を付与して、格納許可証を生成し、該格納許可情報をデータ提供装置に送信させるプロセスとを有する請求項８記載のデータ格納プログラムを格納した記憶媒体。

【請求項１１】　前記利用者装置に搭載される、

前記登録証、前記格納データ情報を前記データ提供装置に送信させるプロセスと、

前記データ提供装置から受信した格納許可証を検証し、取得した格納データと前記格納データ情報との対応付けを検証し、検証結果が正しければ、該格納データを記憶手段に格納するプロセスと、

前記データ提供装置に搭載される、

前記利用者装置から取得した前記登録証を検証し、検証結果が正しければ該登録証及び前記格納データ情報に対して証明情報を付与し、格納許可証を生成し、該利用者装置に送信させるプロセスとを有する請求項８記載のデータ格納プログラムを格納した記憶媒体。

【請求項１２】　前記発行装置に搭載される、

証明情報を付与するために用いる情報を前記発行登録装置に送信させるプロセスと、

前記発行登録装置より取得した発行機関登録証を検証し、検証結果が正しければ、該発行機関登録証を格納しておくプロセスと、

前記利用者装置に対して前記登録証を生成し、該発行機関登録証と共に該利用者装置に送信させるプロセスと、

前記発行登録装置に搭載される、

前記発行装置から受信した前記証明情報を付与するために用いる情報に対して証明情報を付与し、発行機関登録証を作成し、前記発行装置に送信させるプロセスと、

前記利用者装置に搭載される、

前記発行装置から取得した、前記登録証と前記発行機関登録証の両者を検証し、検証結果が正しければ該登録証及び前記発行機関登録証を記憶装置に格納するプロセスとを有する請求項８記載のデータ格納プログラムを格納した記憶媒体。

【請求項１３】　前記データ提供装置に搭載される、

証明情報を付与するために用いる情報を前記データ登録装置に送信させるプロセスと、

前記データ登録装置から受信したデータ提供機関登録証を検証し、検証結果が

正しければ該データ提供機関登録証を格納するプロセスと、

利用者が格納する格納データに対して証明情報を付与して証明情報付き格納データとし、該証明情報付き格納データに前記データ提供機関登録証を付加するプロセスと、

前記データ登録装置に搭載される、

前記データ提供装置から取得した前記証明情報を付与するために用いる情報に対して、証明情報を付与し、データ提供機関登録証を作成して前記データ提供装置に送信させるプロセスと、

前記利用者装置に搭載される、

前記データ提供装置から取得した前記証明情報付き格納データを前記データ提供機関登録証を用いて検証し、検証結果が正しければ前記格納データを前記記憶手段に格納するプロセスとを有する請求項９、１０、または、１１記載のデータ格納プログラムを格納した記憶媒体。

【請求項１４】　前記利用者装置に搭載される、

前記格納データを格納する代わりに、既に前記記憶手段内にある格納データを削除するプロセスを有する請求項９、１０、または、１１記載のデータ格納プログラムを格納した記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、データ格納システム及びデータ格納プログラムを格納した記憶媒体に係り、特に、電気通信システムやＩＣカード等を利用し、プログラム等のデータをＩＣカード等に格納するためのデータ格納システム及びデータ格納プログラムを格納した記憶媒体に関する。

【０００２】

【従来の技術】

昨今、データ格納システムとして、セキュリティ上安全な装置（ＩＣカード等）を利用したシステムが普及しつつある。これらの装置に対してプログラム等の重要なデータの格納は、発行機関（ＩＣカード発行機関）が装置提供時に行って

いる。

【０００３】

【発明が解決しようとする課題】

しかしながら、利用者装置（ＩＣカード等）にプログラムを格納する権限はセキュリティ上の問題により、発行機関（ＩＣカード発行機関）に全て持たせてあるため、プログラムを提供しているデータ提供機関（サービス提供機関）は提供したプログラムを直接利用者に格納させたり、プログラムの格納に関する情報について管理できないという問題がある。

【０００４】

また、利用者が、動的にデータを追加、変更、削除を行う際に、正当な発行機関やデータ提供機関の確認をとれていることを確認する手段がないため、ネットワーク等を介して、データ（プログラム等）を安全に格納することができないという問題がある。

本発明は、上記の点に鑑みなされたもので、利用者、カード発行機関、サービス提供機関がそれぞれ合意して、カード発行機関もサービス提供者も同等に安全にＩＣカードにデータを格納、削除させることが可能なデータ格納システム及びデータ格納プログラムを格納した記憶媒体を提供することを目的とする。

【０００５】

また、更なる本発明の目的は、カード発行機関、サービス提供機関がそれぞれＩＣカードに格納されているデータに関する情報を把握することが可能なデータ格納システム及びデータ格納プログラムを格納した記憶媒体を提供することである。

【０００６】

【課題を解決するための手段】

図１は、本発明の原理構成図である。

本発明（請求項１）は、データを格納する利用者装置２００と、該利用者装置２００の提供及び登録証を発行・管理する発行機関が有する発行装置１００と、データを提供するデータ提供機関が有するデータ提供装置、発行機関を登録・管理する発行登録機関が有する発行登録装置と、該データ提供機関を登録・管理す

るデータ登録機関が有するデータ登録装置からなるデータ格納システムにおいて、

利用者装置２００は、

利用者公開鍵を含む鍵に関する情報である登録情報を生成し、利用者情報と共に発行装置１００へ送信する登録情報生成手段２２０と、

発行装置１００から取得した、登録情報及び利用者情報に対する発行機関の署名情報である登録証を検証し、検証結果が正しければ該登録証を記憶手段３１０に記憶する登録証検証手段３３０とを有し、

発行装置１００は、

登録証を生成し、利用者装置２００に送信する登録証生成手段１２０とを有する。

【０００７】

本発明（請求項２）は、利用者装置において、

登録証と格納データ情報を発行装置に送信する手段と、

発行装置から格納許可証を取得すると、該格納許可証を検証し、取得した格納データと、送信した格納データ情報との対応付けを検証し、検証結果が正しければ該格納データを記憶手段に格納する手段とを有し、

発行装置において、

利用者装置から受信した登録証と格納データ情報を検証し、検証結果が正しければ、登録証及び格納データに対して、証明情報を付与し、格納許可依頼を生成し、該登録証、該格納データ及び格納許可情報をデータ提供装置に送信する手段と、

データ提供装置から取得した格納許可証を検証し、検証結果が正しければ該格納許可証を利用者装置に送信する手段とを有し、

データ提供装置において、

格納許可情報を検証し、検証結果が正しければ格納許可依頼及び格納データ情報に対して証明情報を付与し、格納許可証を生成し、該格納許可証を発行装置に送信する手段を有する。

【０００８】

本発明（請求項３）は、利用者装置において、

登録証、格納データ情報をデータ提供装置に送信する手段と、

データ提供装置から格納許可証を取得し、該格納許可証を検証し、取得した格納データと格納データ情報との対応付けを検証し、検証結果が正しければ該格納データを記憶手段に格納する手段とを有し、

データ提供装置において、

利用者装置から取得した登録証及び格納データ情報を検証し、検証結果が正しければ、該登録証及び該格納データ情報に対して証明情報を付与し、格納許可依頼を作成し、該登録証、該格納データ及び該格納許可依頼を発行装置に送信する手段と、

発行装置から取得した格納許可証を検証し、検証結果が正しければ、該格納許可証を利用者装置に送信する手段を有し、

発行装置において、

格納許可依頼を検証し、検証結果が正しければ、該格納許可依頼及び格納データ情報に対して証明情報を付与して、格納許可証を生成し、該格納許可情報をデータ提供装置に送信する手段を有する。

【０００９】

本発明（請求項４）は、利用者装置において、

登録証、格納データ情報をデータ提供装置に送信する手段と、

データ提供装置から受信した格納許可証を検証し、取得した格納データと格納データ情報との対応付けを検証し、検証結果が正しければ、該格納データを記憶手段に格納する手段とを有し、

データ提供装置において、

利用者装置から取得した登録証を検証し、検証結果が正しければ該登録証及び格納データ情報に対して証明情報を付与した格納許可証を生成し、該利用者装置に送信する手段を有する。

【００１０】

本発明（請求項５）は、発行装置において、

証明情報を付与するために用いる情報を発行登録装置に送信する手段と、

発行登録装置より取得した発行機関登録証を検証し、検証結果が正しければ、該発行機関登録証を格納しておく手段と、

利用者装置に対して登録証を生成し、該発行機関登録証と共に該利用者装置に送信する手段とを有し、

発行登録装置において、

発行装置から受信した証明情報を付与するために用いる情報に対して証明情報を付与し、発行機関登録証を作成し、発行装置に送信する手段を有し、

利用者装置において、

発行装置から取得した、登録証と発行機関登録証の両者を検証し、検証結果が正しければ該登録証及び発行機関登録証を記憶装置に格納する手段とを有する。

【００１１】

本発明（請求項６）は、データ提供装置において、

証明情報を付与するために用いる情報をデータ登録装置に送信する手段と、

データ登録装置から受信したデータ提供機関登録証を検証し、検証結果が正しければ該データ提供機関登録証を格納する手段と、

利用者が格納する格納データに対して証明情報を付与して証明情報付き格納データとし、該証明情報付き格納データにデータ提供機関登録証を付加する手段とを有し、

データ登録装置において、

データ提供装置から取得した証明情報を付与するために用いる情報に対して証明情報を付与したデータ提供機関登録証を作成してデータ提供装置に送信する手段を有し、

利用者装置において、

データ提供装置から取得した証明情報付き格納データをデータ提供機関登録証を用いて検証し、検証結果が正しければ格納データを記憶手段に格納する手段を有する。

【００１２】

本発明（請求項７）は、利用者装置において、

格納データを格納する代わりに、既に記憶手段内にある格納データを削除する

手段を有する。

本発明（請求項８）は、データを格納する利用者装置と、該利用者装置の提供及び登録証を発行・管理する発行機関が有する発行装置と、データを提供するデータ提供機関が有するデータ提供装置、発行機関を登録・管理する発行登録機関が有する発行登録装置と、該データ提供機関を登録・管理するデータ登録機関が有するデータ登録装置からなるシステムにおいて、該利用者装置、該発行装置、該データ提供装置、該発行登録装置、及びデータ登録装置の各々に搭載されるデータ格納プログラムを格納した記憶媒体であって、

利用者装置に搭載される、

利用者公開鍵を含む鍵に関する情報である登録情報を生成し、利用者情報と共に発行装置へ送信させる登録情報生成プロセスと、

発行装置から取得した、登録情報及び利用者情報に対する発行機関の署名情報である登録証を検証し、検証結果が正しければ該登録証を記憶手段に記憶する登録証検証プロセスと、

発行装置に搭載される、

登録証を生成し、利用者装置に送信させる登録証生成プロセスとを有する。

【００１３】

本発明（請求項９）は、利用者装置に搭載される、

登録証と格納データ情報を発行装置に送信させるプロセスと、

発行装置から格納許可証を取得すると、該格納許可証を検証し、取得した格納データと、送信した格納データ情報との対応付けを検証し、検証結果が正しければ該格納データを記憶手段に格納するプロセスと、

発行装置に搭載される、

利用者装置から受信した登録証と格納データ情報を検証し、検証結果が正しければ、登録証及び格納データに対して、証明情報を付与し、格納許可依頼を生成し、該登録証、該格納データ及び格納許可情報をデータ提供装置に送信させるプロセスと、

データ提供装置から取得した格納許可証を検証し、検証結果が正しければ該格納許可証を利用者装置に送信させるプロセスと、

データ提供装置に搭載される、

格納許可情報を検証し、検証結果が正しければ格納許可依頼及び格納データ情報に対して証明情報を付与し、格納許可証を生成し、該格納許可証を発行装置に送信させるプロセスを有する。

【００１４】

本発明（請求項１０）は、利用者装置に搭載される、

登録証、格納データ情報をデータ提供装置に送信させるプロセスと、　データ提供装置から格納許可証を取得し、該格納許可証を検証し、取得した格納データと格納データ情報との対応付けを検証し、検証結果が正しければ該格納データを記憶手段に格納するプロセスと、

データ提供装置に搭載される、

利用者装置から取得した登録証及び格納データ情報を検証し、検証結果が正しければ、該登録証及び該格納データ情報に対して証明情報を付与し、格納許可依頼を作成し、該登録証、該格納データ及び該格納許可依頼を発行装置に送信させるプロセスと、

発行装置から取得した格納許可証を検証し、検証結果が正しければ、該格納許可証を利用者装置に送信させるプロセスと、

発行装置に搭載される、

データ提供装置から取得した格納許可依頼を検証し、検証結果が正しければ、該格納許可依頼及び格納データ情報に対して証明情報を付与して、格納許可証を生成し、該格納許可情報をデータ提供装置に送信させるプロセスとを有する。

【００１５】

本発明（請求項１１）は、利用者装置に搭載される、

登録証、格納データ情報をデータ提供装置に送信させるプロセスと、

データ提供装置から受信した格納許可証を検証し、取得した格納データと格納データ情報との対応付けを検証し、検証結果が正しければ、該格納データを記憶手段に格納するプロセスと、

データ提供装置に搭載される、

利用者装置から取得した登録証を検証し、検証結果が正しければ該登録証及び

格納データ情報に対して証明情報を付与し、格納許可証を生成し、該利用者装置に送信させるプロセスとを有する。

【００１６】

本発明（請求項１２）は、発行装置に搭載される、

証明情報を付与するために用いる情報を発行登録装置に送信させるプロセスと、

発行登録装置より取得した発行機関登録証を検証し、検証結果が正しければ、該発行機関登録証を格納しておくプロセスと、

利用者装置に対して登録証を生成し、該発行機関登録証と共に該利用者装置に送信させるプロセスと、

発行登録装置に搭載される、

発行装置から受信した証明情報を付与するために用いる情報に対して証明情報を付与し、発行機関登録証を作成し、発行装置に送信させるプロセスと、

利用者装置に搭載される、

発行装置から取得した、登録証と発行機関登録証の両者を検証し、検証結果が正しければ該登録証及び発行機関登録証を記憶装置に格納するプロセスとを有する。

【００１７】

本発明（請求項１３）は、データ提供装置に搭載される、

証明情報を付与するために用いる情報をデータ登録装置に送信させるプロセスと、

データ登録装置から受信したデータ提供機関登録証を検証し、検証結果が正しければ該データ提供機関登録証を格納するプロセスと、

利用者が格納する格納データに対して証明情報を付与して証明情報付き格納データとし、該証明情報付き格納データにデータ提供機関登録証を付加するプロセスと、

データ登録装置に搭載される、

データ提供装置から取得した証明情報を付与するために用いる情報に対して、証明情報を付与し、データ提供機関登録証を作成してデータ提供装置に送信させ

るプロセスと、

利用者装置に搭載される、

データ提供装置から取得した証明情報付き格納データをデータ提供機関登録証を用いて検証し、検証結果が正しければ格納データを記憶手段に格納するプロセスとを有する。

【００１８】

本発明（請求項１４）は、利用者装置に搭載される、

格納データを格納する代わりに、既に記憶手段内にある格納データを削除するプロセスを有する。

上記のように、本発明は、利用者装置が登録情報を生成し、利用者情報と共に発行機関へ送信し、発行機関は、受信した登録情報と利用者情報を格納し、登録情報に対して証明情報を付与し、登録証を生成し、利用者層に送信し、利用者装置は受信した登録証を検証し、検証結果が正しければ登録証を記憶手段に記憶する利用者登録を基本として、ＩＣカードのデータを安全にデータを格納・削除するものである。

【００１９】

これにより、発行機関によって発行される登録証により被発行者を保証し、データ格納、削除等の処理をカード発行機関・サービス提供機関の両者が安全に行うことが可能となる。

また、発行機関、データ提供機関、利用者装置で登録証、格納許可依頼、格納許可証を検証することにより、第三者による改竄を防止し、また、格納データ数などの格納されたデータに関する情報を把握することが可能となる。

【００２０】

【発明の実施の形態】

図２は、本発明のデータ格納システムの構成を示す。

同図に示すデータ格納システムは、利用者装置の提供及び、登録証を発行・管理する機関である発行機関が有する発行装置１００、データを提供するデータ提供機関が有するデータ提供装置２００、登録証やデータを格納する利用者装置３００、発行機関を登録・管理し、登録証の正当性を保証する発行登録機関が有す

る発行登録装置４００、データの提供機関を登録・管理し、データの正当性を保証する機関であるデータ登録機関が有するデータ登録装置５００から構成される。

【００２１】

これらの装置間は、何らかのデータのやりとりが行えればよく、例えば、通信回線等を介して接続している場合を表す。また、これらの各装置は、耐タンパ装置（ＩＣカードなど）を用いてもよい。

発行装置１００、データ提供装置２００、発行登録装置４００、データ登録装置５００は、予め共通鍵暗号方式、公開鍵暗号方式、ディジタル署名方式、セキュアハッシュ（メッセージダイジェスト）（池野、小山著「現代暗号理論」電子情報通信学会、等を参照）などを用いている証明書作成用・証明書検証用の鍵情報（公開鍵・秘密鍵・共有鍵等）を生成して保持しているものとする。

【００２２】

【実施例】

以下、図面と共に本発明の実施例を説明する。

［第１の実施例］

本実施例では、利用者装置３００と発行装置１００との間における利用者登録の処理について説明する。

【００２３】

図３は、本発明の第１の実施例の利用者登録時のシステム構成を示す。

同図に示すシステムは、発行装置１００と利用者装置３００から構成される。

同図に示す発行装置１００は、データベース１１０と証明書作成部１２０から構成される。証明書作成部１２０は、入力データに対して発行機関が作成したことを証明するためのディジタル署名（又は、暗号化データ、又は、セキュアハッシュ）を作成する。ここで、入力データとして、利用者装置３００から、利用者公開鍵など鍵に関する情報（公開鍵、共通鍵方式における共有鍵等）（ＵＩ）及び、利用者識別子などからなる利用者情報（ＵＩＤ）が入力されるものとする。証明書作成部１２０は、利用者装置３００から入力された登録情報（ＵＩ）と利用者情報（ＵＩＤ）に対する発行機関のディジタル署名（又は、暗号化データま

たは、セキュアハッシュ）を生成し、これを登録証（Ｌ）として利用者装置３００に出力する。

【００２４】

利用者装置３００は、メモリ３１０、登録情報生成部３２０、及び証明書検証部３３０から構成される。

登録情報生成部３２０は、登録情報（ＵＩ）、及び利用者情報（ＵＩＤ）を生成し、メモリ３１０に格納する。

証明書検証部３３０は、発行装置１００から入力された登録証（Ｌ）の正当性を検証する。登録証（Ｌ）のディジタル署名（又は、暗号化データ、または、セキュアハッシュ）を検証し、正当であれば、当該登録証（Ｌ）をメモリ３１０に格納する。

【００２５】

上記の構成における利用者登録動作は、以下の通りである。

① まず、利用者装置３００が、登録情報生成部３２０を用いて、登録装置１００への登録情報（ＵＩ）を生成し、メモリ３１０に格納し、当該登録情報（ＵＩ）を発行装置１００に送信する。

② 次に、発行装置１００は、受信した登録情報（ＵＩ）を用いて証明書作成部１２０にて、登録証（Ｌ）を作成し、データベース１１０に格納し、登録証（Ｌ）を利用者装置３００に送信する。

【００２６】

③ 利用者装置３００は、証明書検証部３３０において、登録証（Ｌ）を検証し、検証結果が正しければ、登録証（Ｌ）をメモリ３１０に格納する。

［第２の実施例］

本実施例では、発行機関を経由してデータの格納を行う処理について説明する。

【００２７】

図３は、本発明の第２の実施例の発行機関を経由したデータ格納時のシステム構成を示す。

同図に示すシステムは、発行装置１００、データ提供装置２００、及び利用者

装置３００から構成される。

発行装置１００は、証明書作成部１２０、証明書検証部１３０、及び格納データ検証部１４０から構成される。

【００２８】

証明書検証部１３０は、利用者装置３００から登録証（Ｌ）を取得し、当該発行装置１００で作成したことを証明するためのディジタル署名（又は、暗号化データ、又は、セキュアハッシュ）を検証する。検証結果が正当である場合には、格納許可証を発行し、利用者装置３００に転送する。

格納データ検証部１４０は、利用者装置３００から、格納データ識別子などからなる格納データ情報（ＡＩＤ）を取得して、当該データ（ＡＩＤ）の検証を行い、正当であれば、検証結果（格納データ情報（ＡＩＤ））を証明書作成部１２０及びデータ提供装置２００に転送する。

【００２９】

証明書作成部１２０は、証明書検証部１３０から検証済の登録証（Ｌ）と、格納データ検証部１４０から検証済の格納データ情報（ＡＩＤ）を取得して、登録証（Ｌ）と格納データ情報（ＡＩＤ）に対するディジタル署名（又は、暗号化データ又は、セキュアハッシュ）を格納許可依頼（ＤＲ）としてデータ提供装置２００に転送する。

【００３０】

データ提供部２００は、データベース２１０、証明書作成部２２０、証明書検証部２３０、及び格納データ検証部２４０から構成される。

証明書検証部２３０は、発行装置１００から格納許可依頼（ＤＲ）を取得すると、当該格納許可依頼の正当性を検証し、正当であれば、格納データ情報（ＡＩＤ）を格納データ検証部２４０に転送し、格納許可依頼（ＤＲ）を証明書作成部２２０に転送する。

【００３１】

格納データ検証部２４０は、証明書検証部２３０から取得した格納データ情報（ＡＩＤ）をデータベース２１０に書き込むと共に、格納データ情報（ＡＩＤ）を検証して正当であれば、当該格納データ情報（ＡＩＤ）を証明書作成部２２０

に転送する。

証明書作成部２２０は、証明書検証部２３０から取得した格納許可依頼（ＤＲ）と格納データ検証部２４０から取得した格納データ情報（ＡＩＤ）を検証し、正当であれば、格納許可情報（ＤＬ）を発行装置１００に転送する。

【００３２】

利用者装置３００は、メモリ３１０、証明書検証部３３０及び、データ確認部３４０から構成される。

証明書検証部３３０は、発行装置１００から格納許可証（ＤＬ）を取得し、その正当性を検証し、検証結果をデータ確認部３４０に転送する。

データ確認部３４０は、証明書検証部３３０における検証結果が正当である場合に、データ提供装置２１０から格納データ（ＡＰＤ）を取得し、当該格納データ（ＡＰＤ）をメモリ３１０に書き込む。

【００３３】

上記の構成における発行機関を経由したデータ格納時の動作は、以下の通りである。

① 利用者装置３００は、登録証（Ｌ）、格納データ情報（ＡＩＤ）を発行装置１００に送信する。

② 発行装置１００は、証明書検証１３０において、登録証（Ｌ）を検証し、格納データ検証部１４０において、格納データ（ＡＩＤ）を検証し、両者の検証結果が正しければ、送られてきた登録証（Ｌ）、格納データ（ＡＩＤ）に対して、証明書作成部１２０において、格納許可依頼（ＤＲ）を作成し、登録証（Ｌ）、格納データ（ＡＩＤ）、及び格納許可依頼（ＤＲ）をデータ提供装置２００に送信する。

【００３４】

③ データ提供装置２００は、証明書検証部２３０において、格納許可依頼（ＤＲ）を検証し、格納データ検証部２４０において格納データ（ＡＩＤ）を検証し、両方の検証結果が正しければ、格納許可依頼（ＤＲ）、格納データ（ＡＩＤ）に対して証明書作成部２２０において、格納許可証（ＤＬ）を生成し、当該格納許可証（ＤＬ）を発行装置１００に送信する。

【００３５】

④　発行装置１００は、証明書検証部１３０を用いて、格納許可証（ＤＬ）を検証し、検証結果が正しければ、当該格納許可証（ＤＬ）を利用者装置３００に送信する。

⑤　利用者装置３００は、証明書検証部３３０を用いて格納許可証（ＤＬ）を検証し、なんらかの手法により、受領した格納データ（ＡＰＤ）と格納データ情報（ＡＩＤ）との対応付けをデータ確認部３４０を用いて検証し、検証結果が正しければ格納データ（ＡＰＤ）をメモリ３１０に格納する。

【００３６】

なお、上記の処理において、利用者装置３００において、格納データ（ＡＰＤ）を格納する代わりに、既に、メモリ３１０内にある格納データ（ＡＰＤ）を削除することも可能である。

［第３の実施例］

本実施例では、データ提供機関を経由してデータを格納する場合について説明する。

【００３７】

図４は、本発明の第３の実施例のデータ提供機関を経由したデータ格納時のシステム構成を示す。

同図に示すシステムは、発行装置１００、データ提供装置２００、利用者装置３００から構成される。

発行装置１００は、証明書作成部１２０、証明書検証部１３０、及び格納データ検証部１４０から構成される。

【００３８】

証明書検証部１３０は、データ提供装置２００から転送された格納許可依頼（ＤＲ）を取得して、その正当性を検証し、正しければ当該格納許可依頼（ＤＲ）を証明書作成部１２０に転送すると共に、データ提供装置２００から転送された格納データ情報（ＡＩＤ）を格納データ検証部１４０に転送する。

格納データ検証部１４０は、格納データ情報（ＡＩＤ）の正当性を検証し、正しければ、格納データ情報（ＡＩＤ）を証明書作成部１２０に転送する。

【００３９】

証明書作成部１２０は、証明書検証部１３０から転送された格納許可依頼（ＤＲ）と格納データ検証部１４０から取得した格納データ情報（ＡＩＤ）に基づいて当該発行機関が作成したことを証明するためのディジタル署名（または、暗号化データ、又は、セキュアハッシュ）を格納許可証（ＤＬ）としてデータ提供装置２００に転送する。

【００４０】

データ提供装置２００は、データベース２１０、証明書作成部２２０、証明書検証部２３０、格納データ検証部２４０から構成される。

証明書検証部２３０は、発行装置１００から格納許可証（ＤＬ）と、利用者装置３００から登録証（Ｌ）を取得して、これらの正当性を検証する。

証明書作成部２２０は、証明書検証部２３０から取得した登録証（Ｌ）と格納データ検証部２４０から取得した格納データ情報（ＡＩＤ）を用いて格納許可依頼（ＤＲ）を生成し、発行装置１００に転送する。

【００４１】

格納データ検証部２４０は、利用者装置３００から格納データ情報（ＡＩＤ）を取得し、この正当性を検証し、正しければ当該格納データ情報（ＡＩＤ）を証明書作成部２２０に転送する。

利用者装置３００は、メモリ３１０、証明書検証部３３０、及びデータ確認部３４０から構成される。

【００４２】

メモリ３１０から登録証（Ｌ）をデータ提供装置２００の証明書検証部２３０に転送し、格納データ情報（ＡＩＤ）をデータ提供装置２００の格納データ検証部２４０に転送する。

証明書検証部３３０は、データ提供装置２３０の証明書検証部２３０から格納許可証（ＤＬ）を取得し、当該格納許可証（ＤＬ）の正当性を検証し、正しければ、データ確認部３４０にその検証結果を転送する。

【００４３】

データ確認部３４０は、データ提供装置２００のデータベース２１０から格納

データ（ＡＰＤ）を取得し、その正当性を確認し、正しければ、当該格納データ（ＡＰＤ）をメモリ３１０に格納する。

上記の構成におけるデータ提供機関を経由したデータの格納処理について説明する。

【００４４】

① 利用者装置３００は、登録証（Ｌ）、格納データ情報（ＡＩＤ）をデータ提供装置２００に送信する。

② データ提供装置２００は、証明書検証部２３０において、登録証（Ｌ）を検証し、格納データ検証部２４０において格納データ情報（ＡＩＤ）を検証し、両者の検証結果が正しければ、送られてきた登録証（Ｌ）、格納データ（ＡＩＤ）に対して証明書作成部２２０において、格納許可依頼（ＤＲ）を作成し、登録証（Ｌ）、格納データ（ＡＩＤ）、格納許可依頼（ＤＲ）を発行装置１００に送信する。

【００４５】

③ 発行装置１００は、証明書検証部１３０において、格納許可依頼（ＤＲ）を検証し、格納データ検証部１４０において、格納データ（ＡＩＤ）を検証し、両者の検証結果が正しければ、格納許可依頼（ＤＲ）、格納データ（ＡＩＤ）に対して証明書作成部１２０において、格納許可証（ＤＬ）を生成し、当該格納許可証（ＤＬ）をデータ提供装置２００に送信する。

【００４６】

④ データ提供装置２００は、証明書検証部２３０において、格納許可証（ＤＬ）を検証し、検証結果が正しければ、当該格納許可証（ＤＬ）を利用者装置３００に送信する。

⑤ 利用者装置３００は、証明書検証部３３０において、格納許可証（ＤＬ）を検証し、なんらかの手法により受領した格納データ（ＡＰＤ）と格納データ情報（ＡＩＤ）との対応付けをデータ確認部３４０において検証し、検証結果が正しければ、格納データ（ＡＰＤ）をメモリ３１０に格納する。

【００４７】

なお、上記の処理において、利用者装置３００において、格納データ（ＡＰＤ

）を格納する代わりに、既に、メモリ３１０内にある格納データ（ＡＰＤ）を削除することも可能である。

［第４の実施例］

本実施例では、データ提供機関のみによるデータ格納について説明する。

【００４８】

図５は、本発明の第４の実施例のデータ提供機関のみによるデータ格納時のシステム構成を示す。

同図に示すシステムは、データ提供装置２００及び利用者装置３００から構成される。

データ提供装置２００は、データベース２１０、証明書作成部２２０、証明書検証部２３０及び、格納データ検証部２４０から構成される。

【００４９】

証明書検証部２３０は、利用者装置３００から登録証（Ｌ）を取得し、当該登録証の正当性を検証する。

格納データ検証部２４０は、利用者装置２００から格納データ情報（ＡＩＤ）を取得し、その正当性を検証する。

証明書作成部２２０は、登録証（Ｌ）と格納データ情報（ＡＩＤ）の両方の正当性を検証し、検証結果が正しければ、格納許可証（ＤＬ）を作成し、利用者装置３００に送信する。

【００５０】

利用者装置３００は、メモリ３１０、証明書検証部３３０、及びデータ確認部３４０から構成される。

証明書検証部３３０は、データ提供装置２００から取得した格納許可依頼（ＤＬ）を取得し、その正当性を検証する。

データ確認部３４０は、データ提供装置２００から取得した格納データ（ＡＰＤ）を取得して、その正当性を検証し、正しければ当該格納データ（ＡＰＤ）を格納する。

【００５１】

上記の構成におけるデータ提供者のみによるデータ格納時の動作を説明する。

① 利用者装置３００は、登録証（Ｌ）、格納データ情報（ＡＩＤ）をデータ提供装置２００に送信する。

② データ提供装置２００は、証明書検証部２３０において、登録証（Ｌ）を検証し、検証結果が正しければ、格納データ情報（ＡＩＤ）に対して証明書作成部２２０において、格納許可証（ＤＬ）を生成し、当該格納許可証（ＤＬ）を利用者装置３００に送信する。

【００５２】

③ 利用者装置３００は、証明書検証部３３０において、格納許可証（ＤＬを検証し、なんらかの手法により、受領した格納データ（ＡＰＤ）と格納データ情報（ＡＩＤ）との対応付けをデータ確認部３４０を用いて検証し、検証結果が正しければ格納データ（ＡＰＤ）をメモリ３１０に格納する。

なお、上記の処理において、利用者装置３００において、格納データ（ＡＰＤ）を格納する代わりに、既に、メモリ３１０内にある格納データ（ＡＰＤ）を削除することも可能である。

【００５３】

［第５の実施例］

図６は、本発明の第５の実施例の利用者登録時のシステム構成を示す。

同図に示すシステムは、発行装置１００、利用者装置３００、及び、発行登録装置４００から構成される。

発行登録装置４００は、データベース４１０と、証明書作成部４２０から構成される。

【００５４】

証明書作成部４２０は、発行装置１００か取得した発行機関た証明情報を付与するための情報（ＰＫＩ）を取得して、発行機関登録証（ＬＩ）を生成し、データベース４１０に格納すると共に、当該発行機関登録証（ＬＩ）を発行装置１００に送信する。

発行装置１００は、データベース１１０、証明書作成部１２０、証明書検証部１３０、鍵情報生成部１５０から構成される。

【００５５】

証明書作成部１２０は、利用者装置３００から取得した登録情報（ＵＩ）に基づいて登録証（Ｌ）を生成してデータベース１１０に格納すると共に、当該登録証（Ｌ）を利用者装置１００に送信する。

証明書検証部１３０は、発行登録装置４００から取得した発行機関登録証（ＬＩ）を取得して、検証を行い、正しければ、当該発行機関登録証（ＬＩ）をデータベース１１０に格納する。

【００５６】

鍵情報生成部１５０は、発行機関が証明情報を付与するための情報（ＰＫＩ）を生成する。

利用者装置３００は、メモリ３１０、登録情報生成部３２０、証明書検証部３３０から構成される。

登録情報生成部３２０は、利用者公開鍵など鍵に関する情報（ＵＩ）（公開鍵、共通鍵方式における共有鍵等）の登録情報を生成し、メモリ３１０に格納する。

【００５７】

証明書検証部３３０は、発行装置１００から取得した発行機関登録証（ＬＩ）と登録証（Ｌ）を取得して検証し、これらの両方が正しければ、発行機関登録証（ＬＩ）と登録証（Ｌ）をメモリ１１０に格納する。

次に、上記の構成における利用者登録時の動作を説明する。

① 発行装置１００は、証明情報を付与するために用いる（証明書作成部１２０にて用いる）情報（鍵情報）を鍵情報生成部１５０を用いて生成し、その情報（（鍵情報、または、鍵情報の一部）ＰＫＩ）を発行登録装置４００に送信する。

【００５８】

② 発行登録装置４００は、発行機関が証明情報を付与するための情報（ＰＫＩ）に対して証明書作成部４２０において、発行機関登録書（ＬＩ）を作成し、データベース４１０に、発行機関が証明情報を付与するための情報（ＰＫＩ）、発行機関登録証（ＬＩ）を格納し、発行機関登録証（ＬＩ）を発行装置１００に送信する。

【００５９】

③　発行装置１００は、証明書検証部１３０において、発行機関登録証（ＬＩ）を検証し、検証結果が正しければ、当該発行機関登録証（ＬＩ）をデータベース１１０に格納する。

④　利用者装置３００は、登録情報生成部３２０において、登録装置１００への登録情報（ＵＩ）を生成し、メモリ３１０へ格納し、当該登録情報（ＵＩ）を発行装置１００に送信する。

【００６０】

⑤　発行装置１００は、受信した登録情報（ＵＩ）を用いて証明書作成部１２０において、登録証（Ｌ）を作成し、メモリ１１０に格納し、登録証（Ｌ）及び発行機関登録証（ＬＩ）を利用者装置３００に送信する。

⑥　利用者装置３００は、証明書検証部３３０により、登録証（Ｌ）及び発行機関登録証（ＬＩ）を検証し、両者の検証結果が正しければ、登録証（Ｌ）、発行機関登録証（ＬＩ）をメモリ１１０に格納する。

【００６１】

［第６の実施例］

本実施例では、データ登録機関を用いてデータを格納する場合について説明する。

図７は、本発明の第６の実施例のデータ格納時のシステム構成を示す。

同図に示すシステムは、データ提供装置２００、利用者装置３００及び、データ登録装置５００から構成される。

【００６２】

データ登録装置５００は、データベース５１０、証明書作成部５２０から構成される。

証明書作成部５２０は、データ提供装置２００から取得したデータ提供機関が証明情報を付与するための情報（ＰＫＤ）を取得して、当該情報（ＰＫＤ）に対するデータ登録機関のディジタル署名であるデータ提供機関登録証（ＬＤ）を作成し、データベース５１０に格納すると共に、データ提供装置２００に転送する。

【００６３】

データ提供装置２００は、データベース２１０、証明書作成部２２０、証明書検証部２３０、及び鍵情報生成部２５０から構成される。

証明書作成部２２０は、利用者装置３００から格納データ情報（ＡＩＤ）を取得し、データベース２１０から格納データ（ＡＰＤ）を取得して、格納データ（ＡＰＤ）と格納データ（ＡＰＤ）、格納データ情報（ＡＩＤ）に対するデータ提供許可のディジタル署名である証明情報付き格納データ（ＡＰＤＳ）を生成し、利用者装置３００に転送する。

【００６４】

証明書検証部２３０は、データ登録装置５００からデータ提供機関登録証（ＬＤ）を取得して、その正当性を検証する。

利用者装置３００は、メモリ３１０、証明書検証部３３０、データ確認部３４０から構成される。

証明書検証部３３０は、データ提供装置２００からデータ提供機関登録証（ＬＤ）とデータ提供機関のディジタル署名である証明情報付き格納データ（ＡＰＤＳ）とを取得して、両方の正当性を検証し、正しければ、格納データ（ＡＰＤ）をデータ確認部３４０に転送する。

【００６５】

データ確認部３４０は、転送された格納データ（ＡＰＤ）を検証して正しければ、メモリ３１０に格納する。

上記の構成におけるデータ格納時の動作を説明する。

①　データ提供装置２００は、証明情報を付与するために用いる（証明書作成部２２０にて用いる）情報（鍵情報）を鍵情報生成部２５０において生成し、その情報（鍵情報、または、鍵情報の一部）（ＰＫＤ）をデータ登録装置５００に送信する。

【００６６】

②　データ登録装置５００は、データ提供機関が証明情報を付与するための情報（ＰＫＤ）に対して証明書作成部５２０において、データ提供機関登録証（ＬＤ）を作成し、データベース５１０にデータ提供機関が証明情報を付与するため

の情報（ＰＫＤ）、データ提供機関登録証（ＬＤ）を格納し、当該データ提供機関登録証（ＬＤ）をデータ提供装置２００に送信する。

【００６７】

③　データ提供装置２００は、証明書検証部２３０において、データ提供機関登録証（ＬＤ）を検証し、検証結果が正しければ、データ提供機関登録証（ＬＤ）をデータベース２１０に格納する。

④　利用者装置３００は、格納したいデータに関する格納データ情報（ＡＩＤ）をデータ提供装置２００に送信する。

【００６８】

⑤　データ提供装置２００は、受信した格納データ情報（ＡＩＤ）を用いて、データベース２１０より、必要となるデータ情報（ＡＰＤ）を取得し、証明書作成部２２０において、格納データ情報（ＡＩＤ）と格納データ（ＡＰＤ）に関する証明情報である証明情報付き格納データ（ＡＰＤＳ）を作成し、証明情報付き格納データ（ＡＰＤＳ）とデータ提供機関登録証（ＬＤ）を利用者装置３００に送信する。

【００６９】

⑥　利用者装置３００は、証明書検証部３３０において、証明情報付き格納データ（ＡＰＤＳ）とデータ提供機関登録証（ＬＤ）を検証し、両者の検証結果が正しければ、証明情報付き格納データ（ＡＰＤＳ）から取り出した格納データ（ＡＰＤ）をデータ確認部３４０に送り、要求した格納データ情報（ＡＩＤ）との対応付けをデータ格納部３４０を用いて検証し、検証結果が正しければ格納データ（ＡＰＤ）をメモリ３１０に格納する。

【００７０】

また、上記の実施例は、図３～図８の各構成要素に基づいて説明しているが、利用者装置、データ提供装置、データ登録装置、発行装置、発行登録装置の各構成要素をプログラムとして構築し、利用者装置、データ提供装置、データ登録装置、発行装置、発行登録装置として利用されるコンピュータに接続されるディスク装置や、フロッピーディスク、ＣＤ－ＲＯＭ等の可搬記憶媒体に格納しておき、本発明を実施する際にインストールすることにより、容易に本発明を実現でき

る。

【００７１】

なお、本発明は、上記の実施例に限定されることなく、特許請求の範囲内で種々変更・応用が可能である。

【００７２】

【発明の効果】

上述のように、本発明によれば、以下のような効果を奏する。

（１）　発行機関によって発行される登録証により被発行者を保証し、データ格納、削除等の処理をカード発行機関、サービス提供機関の両者が安全に行うことができる。

【００７３】

（２）　また、利用者、カード発行機関、サービス提供機関がそれぞれ合意して、カード発行機関もサービス提供者も同等に、安全にＩＣカードにデータを格納、削除することができる。

（３）　カード発行機関、サービス提供機関がそれぞれＩＣカードに格納されているデータに関する情報を把握することができる。

【図面の簡単な説明】

【図１】

本発明の原理構成図である。

【図２】

本発明のデータ格納システムの構成図である。

【図３】

本発明の第１の実施例の利用者登録時におけるシステム構成図である。

【図４】

本発明の第２の実施例の発行機関を経由したデータ格納時のシステム構成図である。

【図５】

本発明の第３の実施例のデータ提供機関を経由したデータ格納時のシステム構成図である。

【図６】

本発明の第４の実施例のデータ提供機関のみによるデータ格納時のシステム構成図である。

【図７】

本発明の第５の実施例の利用者登録時のシステム構成図である。

【図８】

本発明の第６の実施例のデータ格納時のシステム構成図である。

【符号の説明】

１００　発行装置
１１０　データベース
１２０　証明書作成部
１３０　証明書検証部
１４０　格納データ検証部
１５０　鍵情報生成部
２００　データ提供装置
２１０　データベース
２２０　証明書作成部
２３０　証明書検証部
２４０　格納データ検証部
２５０　鍵情報生成部
３００　利用者装置
３１０　メモリ
３２０　登録情報生成部
３３０　証明書検証部
３４０　データ確認部
４００　発行登録装置
４１０　データベース
４２０　証明書作成部
５００　データ登録装置

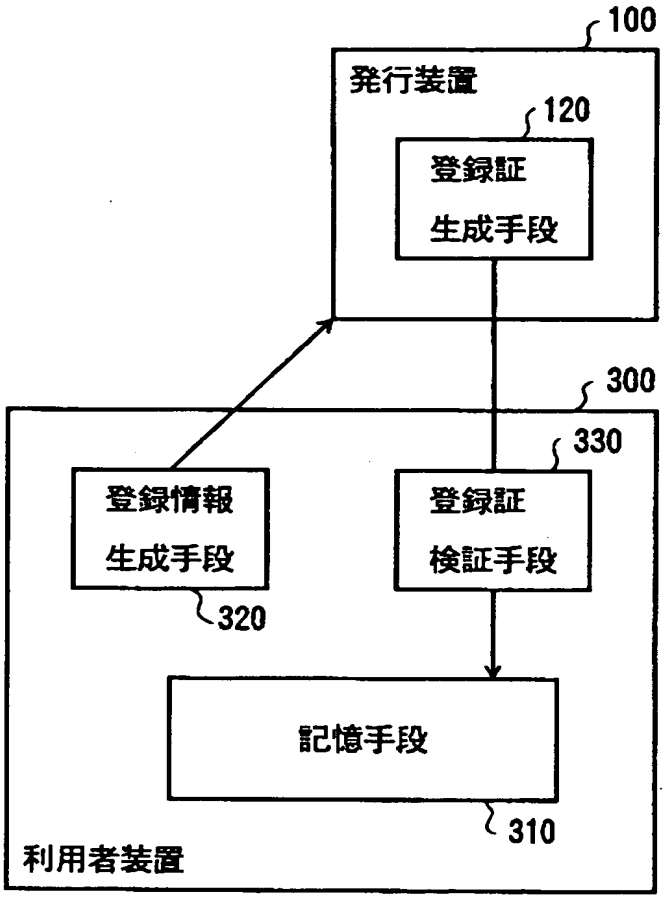
５１０　データベース

５２０　証明書作成部

【書類名】　図面

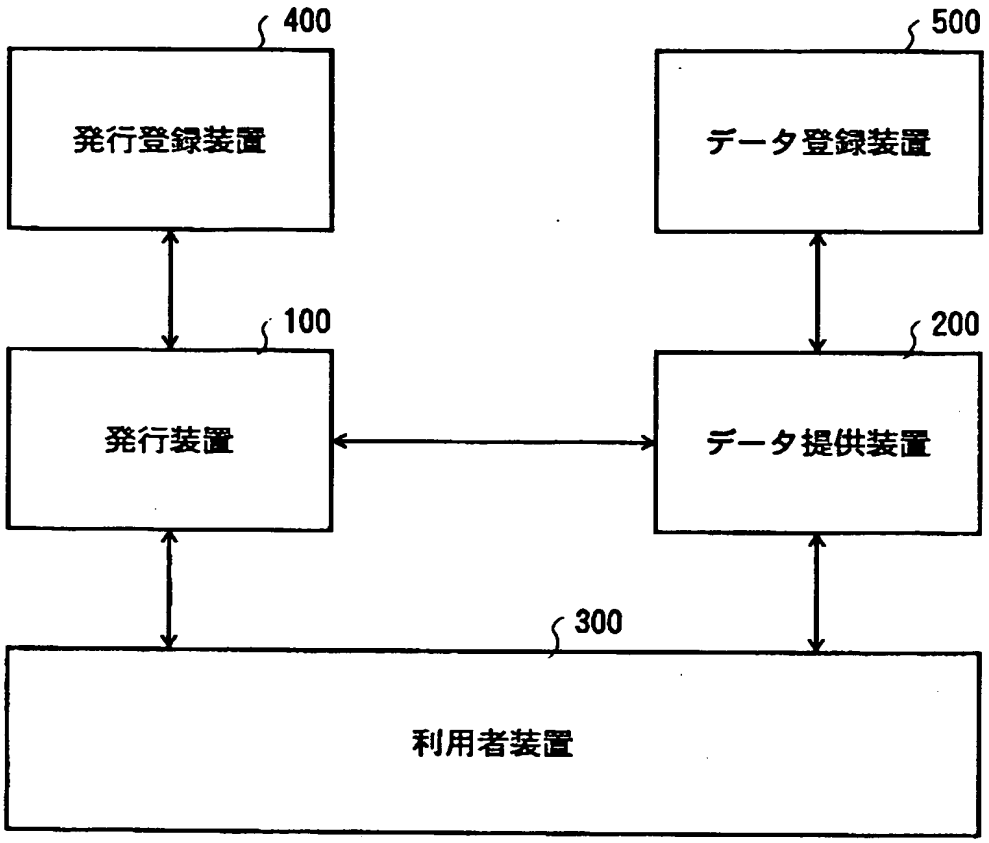
【図１】

本発明の原理構成図



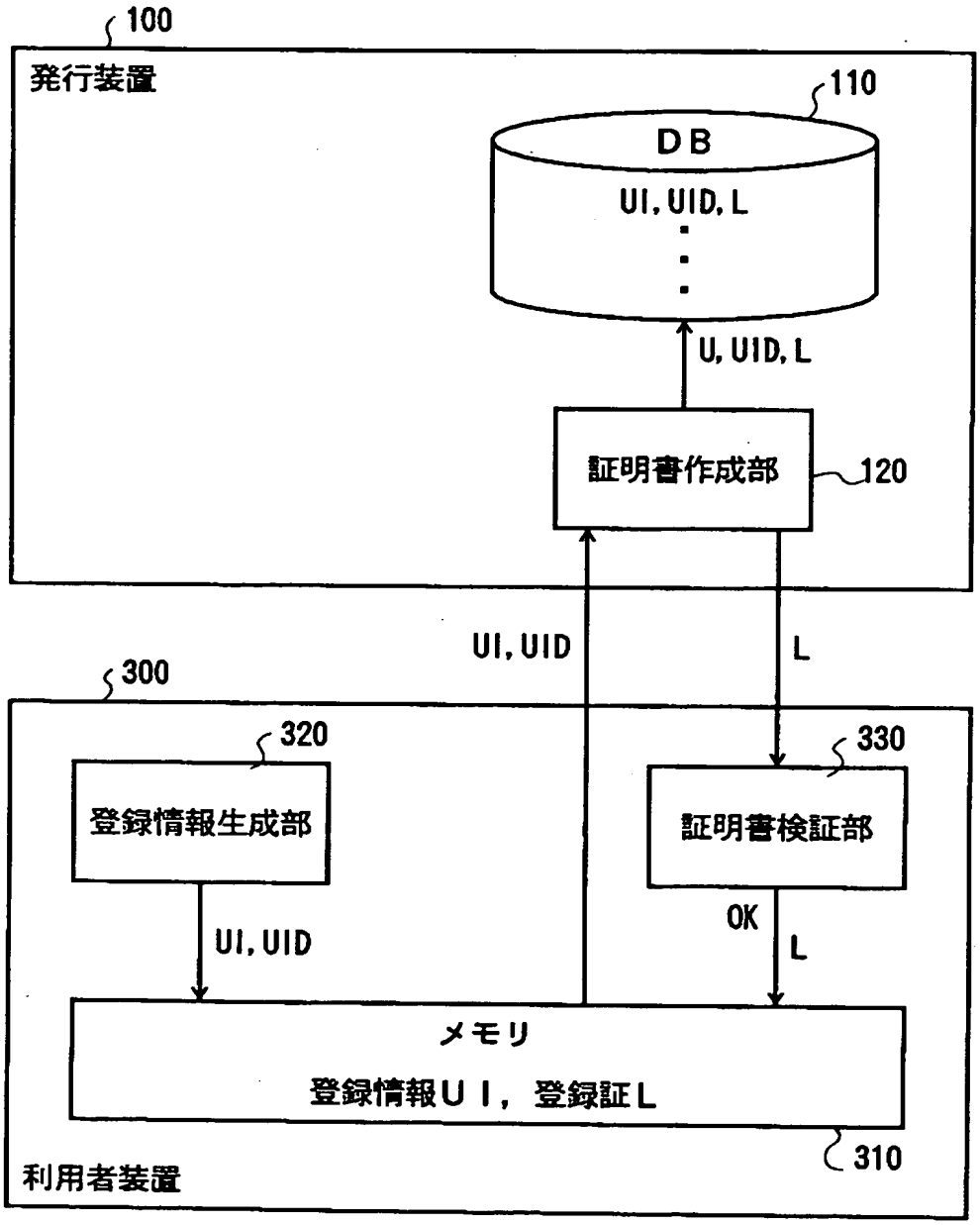
【図２】

本発明のデータ格納システムの構成図



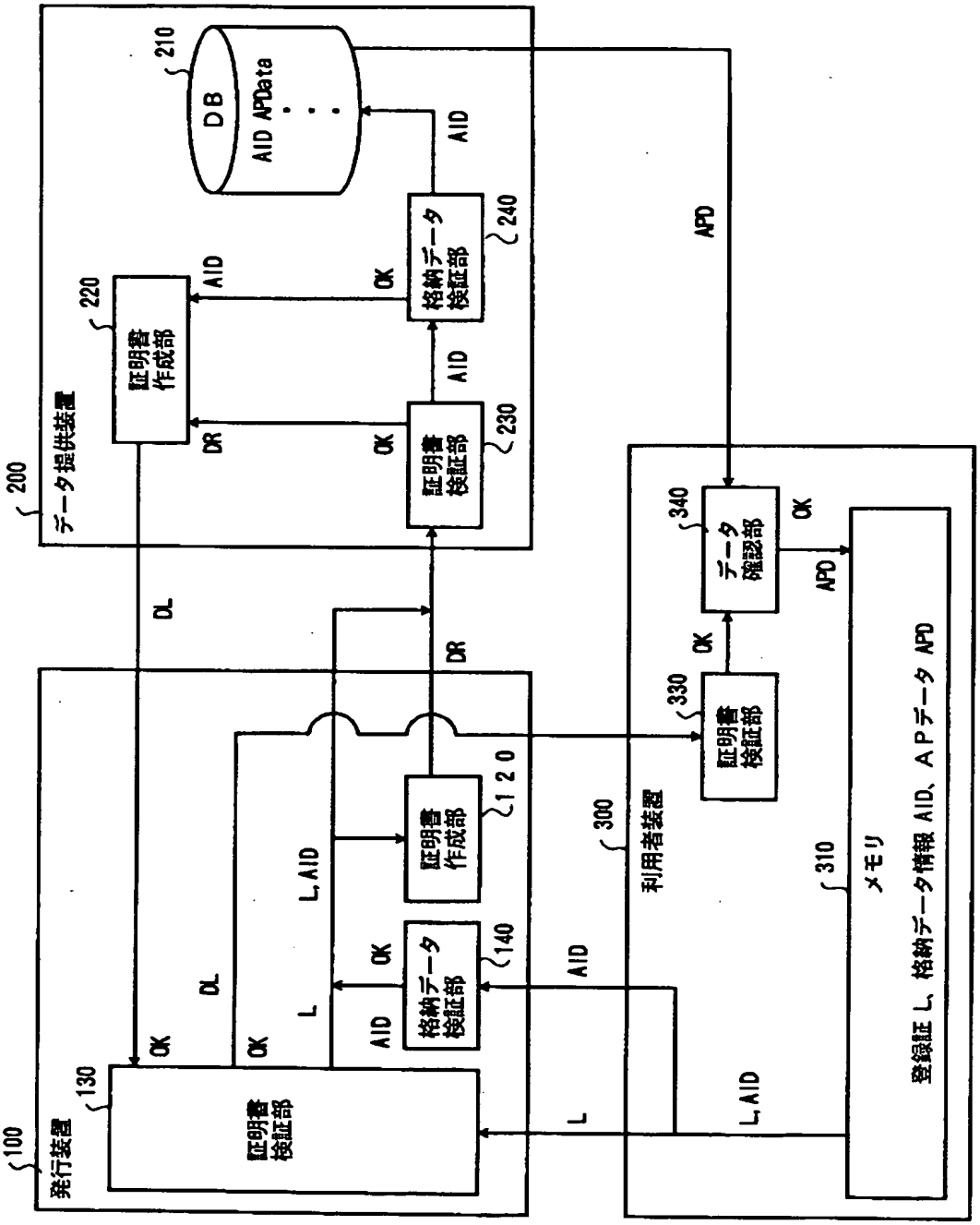
【図３】

本発明の第１の実施例の
利用者登録時におけるシステム構成図



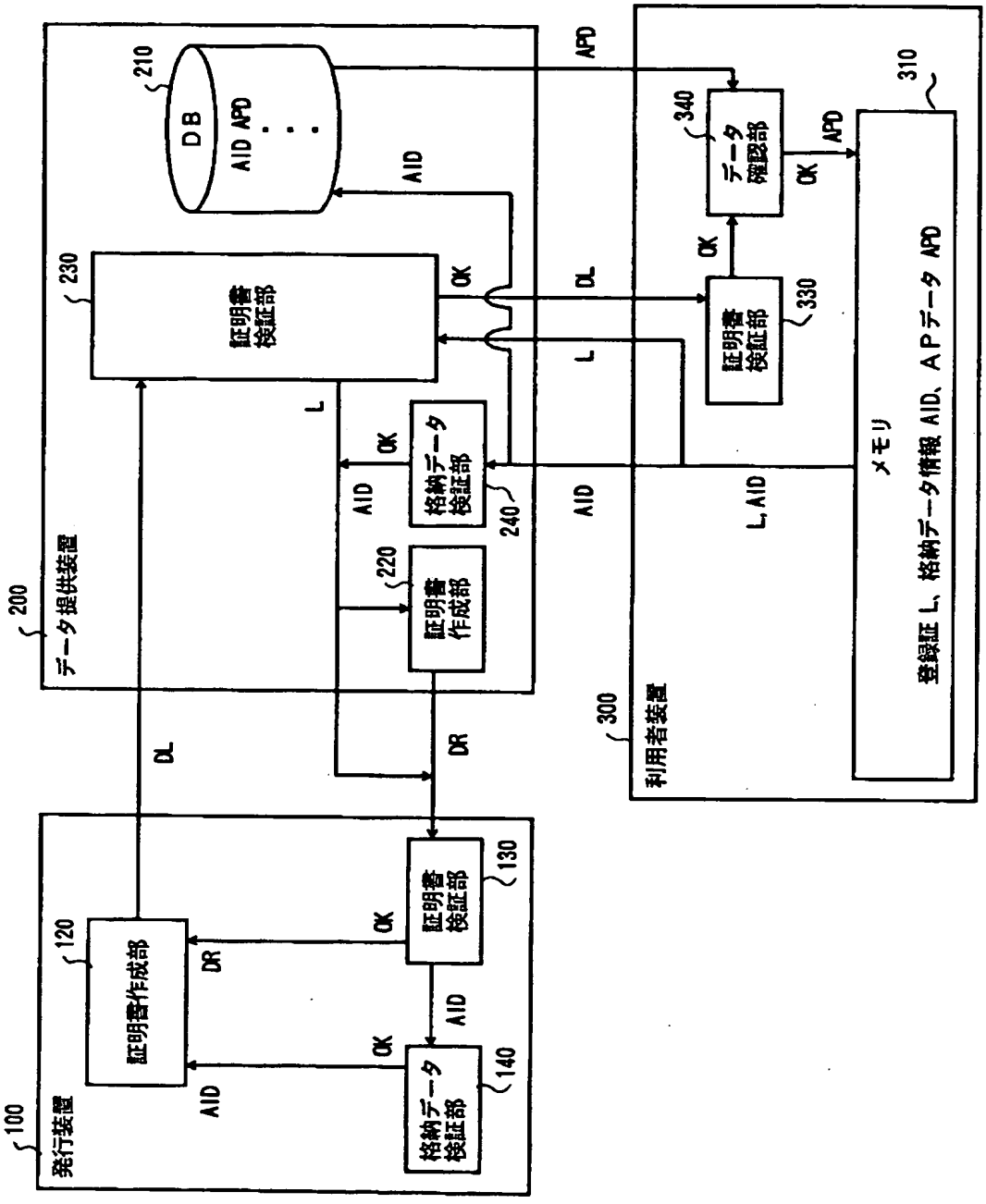
【図４】

本発明の第２の実施例の発行機関を経由した
データ格納時のシステム構成図



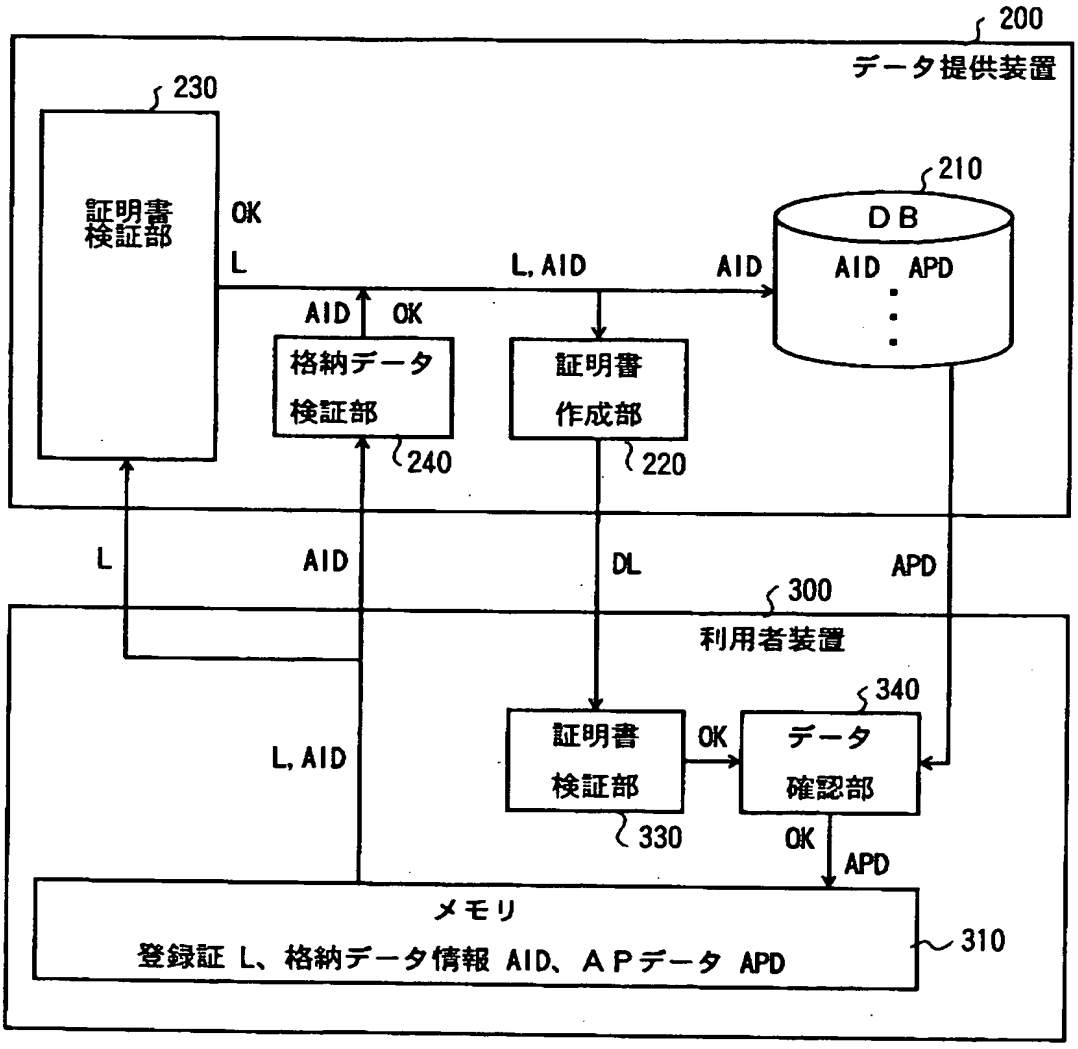
【図５】

本発明の第３の実施例のデータ提供機関を経由したデータ格納時のシステム構成図



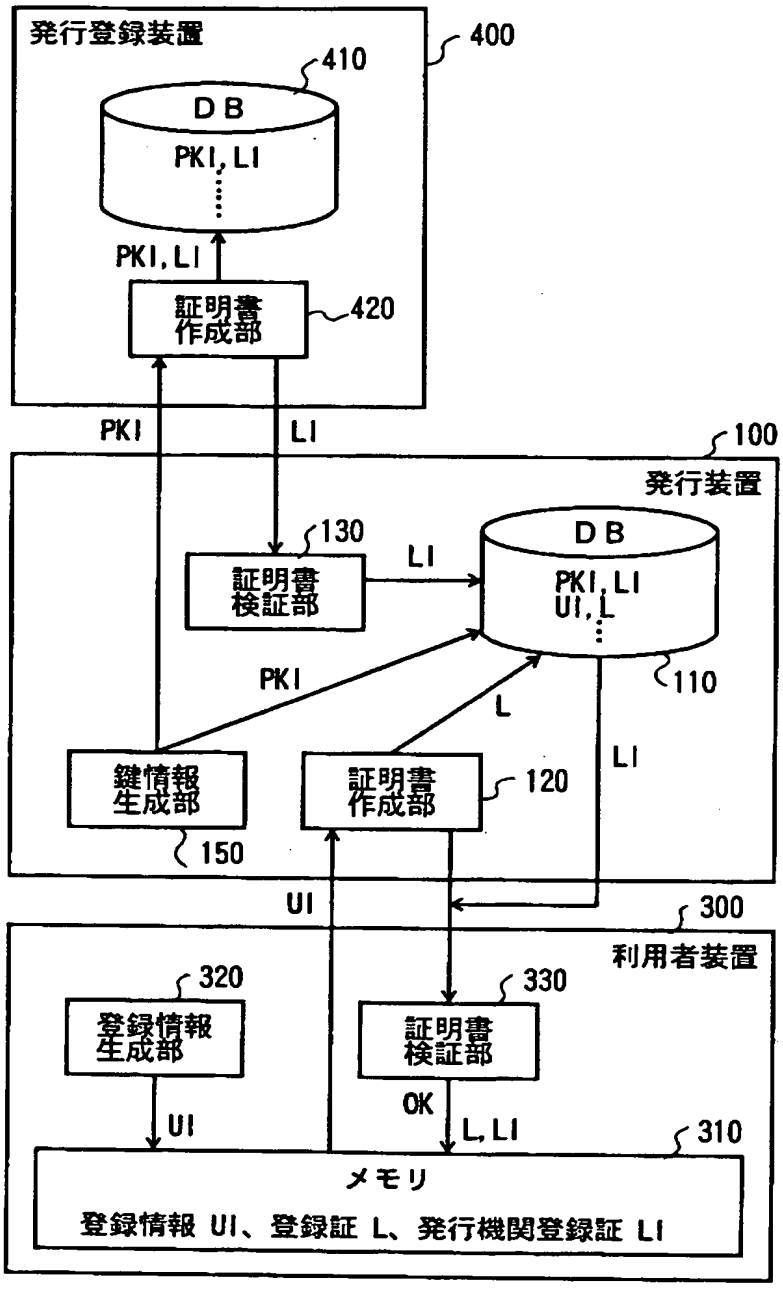
【図６】

本発明の第４の実施例のデータ提供機関のみによるデータ格納時のシステム構成図



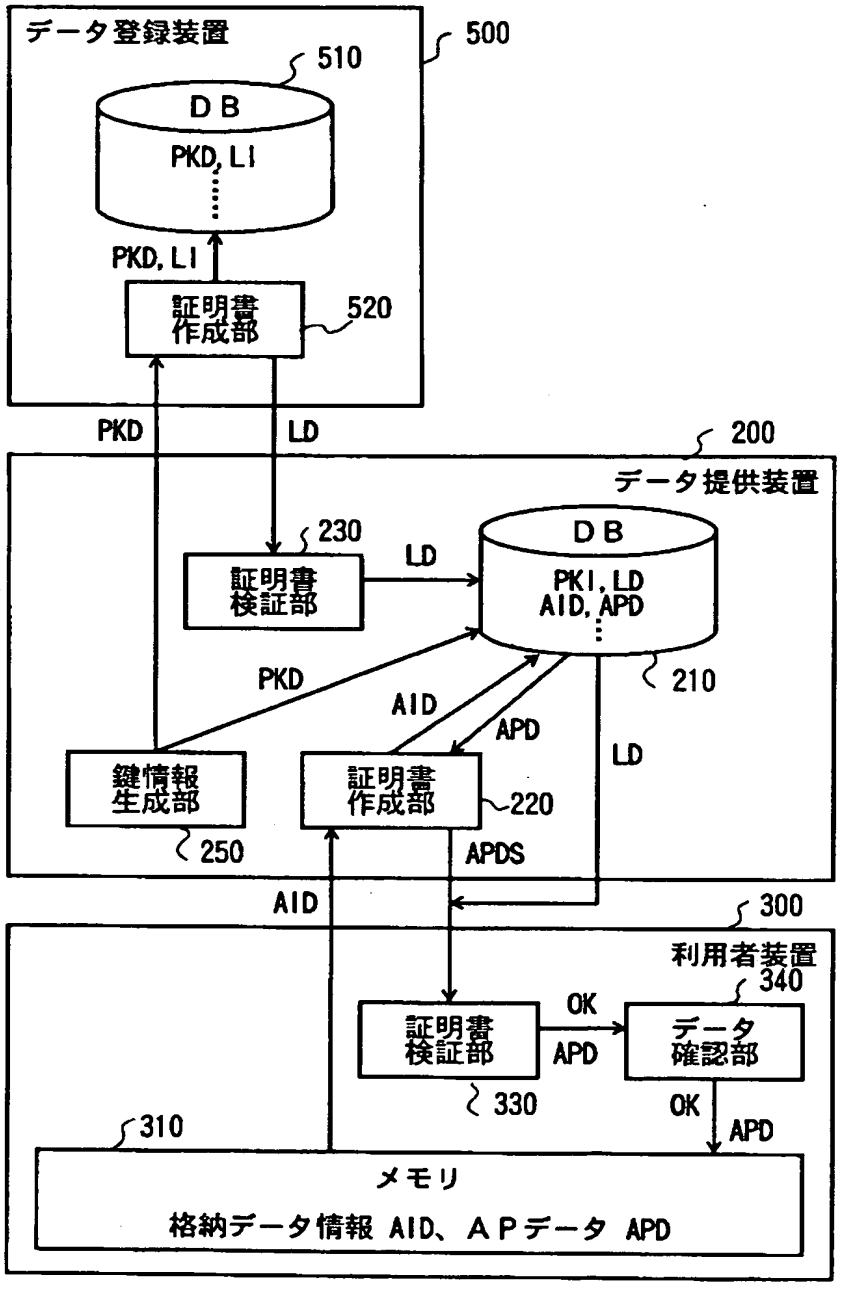
【図７】

本発明の第５の実施例の利用者登録時のシステム構成図



【図８】

本発明の第６の実施例のデータ格納時のシステム構成図



【書類名】　　要約書

【要約】

【課題】　利用者、カード発行機関、サービス提供機関がそれぞれ合意して、カード発行機関もサービス提供者も同等に安全にＩＣカードにデータを格納、削除させることが可能なデータ格納システム及びデータ格納プログラムを格納した記憶媒体を提供する。

【解決手段】　本発明は、利用者装置が登録情報を生成し、利用者情報と共に発行機関へ送信し、発行機関は、受信した登録情報と利用者情報を格納し、登録情報に対して証明情報を付与し、登録証を生成し、利用者層に送信し、利用者装置は受信した登録証を検証し、検証結果が正しければ登録証を記憶手段に記憶する利用者登録を基本として、ＩＣカードのデータを安全にデータを格納・削除する。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００４２２６〕

１．変更年月日　　１９９９年　７月１５日
［変更理由］　住所変更
住　所　　東京都千代田区大手町二丁目３番１号
氏　名　　日本電信電話株式会社

出　願　人　履　歴　情　報

識別番号　　〔５９６０６２７３８〕

１．変更年月日　　１９９６年　３月２９日
［変更理由］　新規登録
住　所　　東京都港区三田１－４－２８
氏　名　　財団法人ニューメディア開発協会